The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should **not** be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product’s vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled “Low” severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Advanced Communications Hosting Controller 6.1	A vulnerability has been reported in Hosting Controller that could let remote malicious users disclose sensitive user information. No workaround or patch available at time of publishing. There is no exploit code required.	Hosting Controller Information Disclosure CVE-2006-1764	Not Available	Secunia, Advisory: SA19569, April 7, 2006
GlobalSCAPE Secure FTP Server 2.0, 3.0 through 3.1.3 various builds	A vulnerability has been reported in GlobalSCAPE Secure FTP server that could let remote malicious users cause a Denial of Service. GlobalSCAPE Secure FTP Server 3.1.4 Build 01.10.2006 Currently we are not aware of any exploits for this vulnerability.	GlobalSCAPE Secure FTP Server Denial of Service CVE-2006-1693	2.3	Secunia, Advisory: SA19547 , April 6, 2006

Microsoft FrontPage Server Extensions	A vulnerability has been reported in FrontPage Server Extensions that could let remote malicious users conduct Cross-Site Scripting. Microsoft There is no exploit code required.	Microsoft FrontPage Server Extensions Cross-Site Scripting CVE-2006-0015	7.0	Microsoft, Security Bulletin MS06-017, April 11, 2006
Microsoft Internet Explorer	Multiple vulnerabilities have been reported in Internet Explorer that could let remote malicious users execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Internet Explorer Arbitrary Code Execution CVE-2006-1185 CVE-2006-1186 CVE-2006-1188 CVE-2006-1189 CVE-2006-1190 CVE-2006-1191 CVE-2006-1192 CVE-2006-1245 CVE-2006-1359 CVE-2006-1388	7.0 (CVE-2006-1185) 10 (CVE-2006-1186) 7.0 (CVE-2006-1188) 10 (CVE-2006-1189) 10 (CVE-2006-1190) 3.7 (CVE-2006-1191) 1.9 (CVE-2006-1192) 7.0 (CVE-2006-1245) 7.0 (CVE-2006-1359) 7.0 (CVE-2006-1388)	Microsoft, Security Bulletin MS06-013, April 11, 2006 US-CERT VU#434641, VU#503124, VU#341028, VU#824324, VU#959649, VU#984473, **VU#959049**, **VU#876678** National Cyber Alert System SA06-101A Technical Cyber Security Alert TA06-101A
Microsoft Microsoft Data Access Components (MDAC)	A vulnerability has been reported in Microsoft Data Access Components (MDAC) that could let remote malicious users execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Data Access Components Arbitrary Code Execution CVE-2006-0003	4.7	Microsoft, Security Bulletin MS06-014, April 11, 2006
Microsoft Outlook Express	A vulnerability has been reported in Outlook Express that could let remote malicious users execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Outlook Express Arbitrary Code Execution CVE-2006-0014	7.0	Microsoft, Security Bulletin MS06-016, April 11, 2006 US-CERT VU#234812
Microsoft Windows Explorer	A vulnerability has been reported in Windows Explorer, COM Object handling, that could let remote malicious users execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Explorer Arbitrary Code Execution CVE-2006-0012	7.0	Microsoft, Security Bulletin MS06-015, April 11, 2006 US-CERT VU#641460
Sony SunnComm MediaMax 5.0.21.0	A vulnerability has been reported due to insecure default directory ACLs set on the 'SunnComm Shared' directory, which could let a malicious user obtain elevated privileges. Patch available Sony Entry erroneously listed as Multiple OS. There is no exploit code required.	Sony SunnComm MediaMax Insecure Directory Permissions CVE-2005-4069	4.9	Secunia Advisory: SA17933, December 7, 2005 Security Tracker, Alert ID: 1015327, December 8, 2005 **US-CERT VU#928689**

TalentSoft Web+ Shop 5.0	An input validation vulnerability has been reported in Web+ Shop that could let remote malicious users conduct Cross-Site Scripting. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Web+ Shop Cross-Site Scripting CVE-2006-1682	2.3	Security Focus, ID: 17418, April 7, 2006
TUGZip 3.1.2, 3.3, 3.4	An input validation vulnerability has been reported in TUGZip that could let remote malicious users to arbitrarily traverse directories. No workaround or patch available at time of publishing. There is no exploit code required.	TUGZip Directory Traversal CVE-2006-1715	2.0	Security Focus, ID: 17432, April 10, 2006

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
Cherokee Cherokee HTTPD 0.5. 0.4.17, 0.4.6 - 0.4.9, 0.2.5-0.2.7, 0.1.6, 0.1.5, 0.1	A Cross-Site Scripting vulnerability has been reported in 'cherokee/handler_error.c' due to insufficient sanitization of the 'build_hardcoded_ response_page()' function before returning to users, which could let a remote malicious user execute arbitrary HTML and script code. Update to version 0.5.1 or later. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Cherokee Webserver Cross-Site Scripting CVE-2006-1681	2.3	Secunia Advisory: SA19587, April 10, 2006
Cyrus SASL Cyrus SASL Library 2.x	A remote Denial of Service vulnerability has been reported due to an unspecified error during DIGEST-MD5 negotiation. Update to version 2.1.21. Currently we are not aware of any exploits for this vulnerability.	Cyrus SASL Remote Digest-MD5 Denial of Service CVE-2006-1721	4.9	Secunia Advisory: SA19618, April 11, 2006
Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported when automatic database configuration is selected during the configuration process because the database administrator password is stored in the world-readable file '/var/cache/debconf/config.dat' which could lead to the disclosure of sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Debian mnoGoSearch-Insecure Password CVE-2006-1772	Not Available	Security Focus, Bugtraq ID: 17477, April 11, 2006
fbida fbida 2.03, 2.01	A vulnerability has been reported in the 'fbgs' script because temporary files are created insecurely when the 'TMPDIR' environment variable isn't defined, which could let a remote malicious user create/overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	Fbida FBGS Insecure Temporary File Creation CVE-2006-1695	1.3	Secunia Advisory: SA19559, April 10, 2006

GNU Mailman 2.1.7	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to the private archive script before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Update available Vulnerability can be exploited through a web client.	Mailman Private Archive Cross-Site Scripting CVE-2006-1712	1.9	Security Tracker Alert ID: 1015876, April 7, 2006
Hewlett Packard Company HP-UX B.11.11	A vulnerability has been reported in the 'su' program when used with the LDAP netgroup feature, which could let a malicious user obtain elevated privileges. Patch available Currently we are not aware of any exploits for this vulnerability.	HP-UX 'SU' Elevated Privileges CVE-2006-1689	7.0	HP Security Bulletin, HPSBUX02111, April 6, 2006
Kaffeine Kaffeine Media Player 0.4.2-0.7.1	A buffer overflow vulnerability has been reported in the 'http_peek()' function when creating HTTP request headers for retrieving remote playlists, which could let a remote malicious user execute arbitrary code. Patches available Debian Mandriva Gentoo **SuSE** **Ubuntu** Currently we are not aware of any exploits for this vulnerability.	Kaffeine Buffer Overflow CVE-2006-0051	5.6	KDE Security Advisory, April 4, 2006 Debian Security Advisory, DSA-1023-1, April 5, 2006 Mandriva Linux Security Advisory MDKSA-2006:065, April 5, 2006 Gentoo Linux Security Advisory, GLSA 200604-04, April 5, 2006 **SUSE Security Summary Report Announcement, SUSE-SR:2006:008, April 7, 2006** **Ubuntu Security Notice, USN-268-1 April 6, 2006**
Manic Web Manic Web MWNewsletter 1.0 b	Multiple vulnerabilities have been reported: a vulnerability was reported in 'subscribe.php' due to insufficient sanitization of the 'user_name' parameter before saving, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported in 'unsubscripbe.php' due to insufficient sanitization of the 'user_name' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and an SQL injection vulnerability was reported in 'unsubscribe.php' due to insufficient sanitization of the 'user_email' parameter and in 'subscribe.php' due to insufficient sanitization of the 'user_name' and 'user_email' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities could be exploited with a web client.	Manic Web MWNewsletter Multiple Input Validation CVE-2006-1690 CVE-2006-1691	7 (CVE-2006-1690) 7.0 (CVE-2006-1691)	Secunia Advisory: SA19568, April 7, 2006

MPlayer MPlayer 1.0.20060329	Multiple vulnerabilities have been reported due to integer overflow errors in 'libmpdemux/asfheader.c' when handling an ASF file, and in 'libmpdemux/aviheader.c' when parsing the 'indx' chunk in an AVI file, which could let a remote malicious user cause a Denial of Service and potentially compromise a system. **MDKSA-2006:068** Currently we are not aware of any exploits for these vulnerabilities.	MPlayer Multiple Integer Overflows CVE-2006-1502	**5.6**	Secunia Advisory: SA19418, March 29, 2006 **Mandriva Security Advisory, MDKSA-2006:068, April 7, 2006**

Multiple Vendors
Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;
MandrakeSoft Linux Mandrake 10.2 x86_64, 10.2, Corporate Server 3.0 x86_64, 3.0;
GNU Mailman 2.1-2.1.5, 2.0-2.0.14, 1.0, 1.1; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha
	A remote Denial of Service vulnerability has been reported in the attachment-scrubber utility.
	Update to version 2.1.6 or later.
	Mandriva
	Ubuntu
	Debian
	SuSE
	There is no exploit code required.
		GNU Mailman Attachment Scrubber Remote Denial of Service
		CVE-2006-0052
			2.3	Security Focus, Bugtraq ID: 17311, March 29, 2006
				Mandriva Security Advisory, MDKSA-2006:061, March 29, 2006
				Ubuntu Security Notice, USN-267-1, April 03, 2006
				Debian Security Advisory, DSA-1027-1, April 6, 2006
				SUSE Security Summary Report Announcement, SUSE-SR:2006:008, April 7, 2006

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3, 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian FreeBSD Gentoo SUS Ubuntu Mandriva OpenBSD OpenPKG RedHat Trustix Slackware TurboLinux Fedora zsync Apple SCO IPCop Debian Trolltech FedoraLegacy Gentoo Debian Trustix Sun Mandriva Ubuntu Ubuntu SCO **dsa-1026** **MDKSA-2006:070** Currently we are not aware of any exploits for this vulnerability.	Zlib Compression Library Buffer Overflow CVE-2005-2096	8.0	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 US-CERT VU#680620 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005

Security Focus, Bugtraq ID: 14162, September 12, 2005

Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005

Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005

Debian Security Advisory, DSA 797-2, September 29, 2005

Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005

Sun(sm) Alert Notification Sun Alert ID: 101989, October 14, 2005

Mandriva Linux Security Advisory MDKSA-2005:196, October 26, 2005

Ubuntu Security Notice, USN-151-3, October 28, 2005

Ubuntu Security Notice, USN-151-4, November 09, 2005

SCO Security Advisory, SCOSA-2006.6, January 10, 2006

Debian Security Advisory, DSA-1026-1, April 6, 2006

Mandriva Security Advisory, MDKSA-2006:070, April 10, 2006

Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib Debian Ubuntu OpenBSD Mandriva Fedora Slackware FreeBSD SUSE Gentoo Gentoo Trustix Conectiva Apple TurboLinux SCO Debian Trolltech FedoraLegacy Debian Mandriva Ubuntu Ubuntu SCO glsa-200603-18 **dsa-1026** **MDKSA-2006:070** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CVE-2005-1849	3.3	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announce-ment, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory, TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 Security Focus, Bugtraq ID: 14340, September 12, 2005 Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005 Debian Security Advisory, DSA 797-2, September 29, 2005 Mandriva Linux Security Advisory, MDKSA-2005:196, October 26, 2005 Ubuntu Security Notice,

				USN-151-3, October 28, 2005 Ubuntu Security Notice, USN-151-4, November 09, 2005 SCO Security Advisory, SCOSA-2006.6, January 10, 2006 Gentoo Linux Security Advisory, GLSA 200603-18, March 21, 2006 **Debian Security Advisory, DSA-1026-1, April 6, 2006** **Mandriva Security Advisory, MDKSA-2006:070, April 10, 2006**
Multiple Vendors Debian Linux 3.1 sparc Debian Linux 3.1 s/390 Debian Linux 3.1 ppc Debian Linux 3.1 mipsel Debian Linux 3.1 mips Debian Linux 3.1 m68k Debian Linux 3.1 ia-64 Debian Linux 3.1 ia-32 Debian Linux 3.1 hppa Debian Linux 3.1 arm Debian Linux 3.1, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; bsd-games bsd-games 2.12-2.14, 2.9, 2.17	Multiple buffer overflow vulnerabilities have been reported due to insufficient bounds-checking when copying user-supplied input to insufficiently sized memory buffers, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	BSD-Games Buffer Overflows CVE-2006-1744	4.9	Security Focus, Bugtraq ID: 17401, April 7, 2006
Multiple Vendors Linux Kernel 2.4, 2.6	A race condition vulnerability has been reported in ia32 emulation, that could let local malicious users obtain root privileges or create a buffer overflow. Patch Available Trustix SUSE RedHat Debian SmoothWall **SGI** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Race Condition and Buffer Overflow CVE-2005-1768	5.6	Security Focus, 14205, July 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 Debian Security Advisory, DSA 921-1, December 14, 2005 SmoothWall Advisory, March 15, 2006 **SGI Security Advisory, 20060402-01-U, April 10, 2006**

Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available Trustix Ubuntu RedHat Avaya SUSE Trustix Mandriva Conectiva SmoothWall **SGI** An exploit script has been published.	Linux Kernel ELF Core Dump Buffer Overflow CVE-2005-1263	7.0	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005 Avaya Security Advisory, ASA-2005-120, June 3, 2005 Trustix Secure Linux Bugfix Advisory, TSLSA-2005-0029, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:110 & 111, June 30 & July 1, 3005 Conectiva Linux Announcement, CLSA-2005:999, August 17, 2005 SmoothWall Advisory, March 15, 2006 **SGI Security Advisory, 20060402-01-U, April 10, 2006**
Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available Fedora Trustix Fedora RedHat Conectiva FedoraLegacy SUSE **SGI** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Local Denial of Service CVE-2005-0749	2.3	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005 SUSE Security Announcement, SUSE-SA:2005:29, June 9, 2005 **SGI Security Advisory, 20060402-01-U, April 10, 2006**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1-test11, 2.6, 2.6.1-2.6.11; RedHat	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability was reported in 'nls_ascii.c' due to the use of incorrect table sizes; a	Linux Kernel Multiple Vulnerabilities CVE-2005-0176 CVE-2005-0177	3.3 (CVE-2005-0176) 3.3 (CVE-2005-0177)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14,

Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	race condition vulnerability was reported in the 'setsid()' function; and a vulnerability was reported in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat Ubuntu Conectiva SUSE Fedora Conectiva Fedora RedHat RedHat RedHat RedHat Avaya FedoraLegacy RedHat Mandriva Trustix **SGI** Currently we are not aware of any exploits for these vulnerabilities.	CVE-2005-0178 CVE-2005-0204	2.3 (CVE-2005-0178) 4.9 (CVE-2005-0204)	February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005 :283-15 & RHSA-2005:284-11, April 28, 2005 RedHat Security Advisory, RHSA-2005: 472-05, May 25, 2005 Avaya Security Advisory, ASA-2005-120, June 3, 2005 FedoraLegacy: FLSA:152532, June 4, 2005 RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005 Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005 Trustix Secure Linux Security Advisory, 2006-0006, February 10, 2006 **SGI Security Advisory, 20060402-01-U, April 10, 2006**
Multiple Vendors Linux Kernel 2.6.x	A Denial of Service vulnerability has been reported in the '_keyring_search_one()' function when a key is added to a non-keyring key. Update to version 2.6.16.3 or later. Currently we are not aware of any exploits for this vulnerability.	Linux Kernel '__keyring_ search_one' Denial of Service CVE-2006-1522	2.3	Secunia Advisory: SA19573, April 11, 2006

Multiple Vendors Linux kernel 2.6-2.6.12, 2.4-2.4.31	A remote Denial of Service vulnerability has been reported due to a design error in the kernel. The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue. Ubuntu Mandriva SUSE Conectiva RedHat RedHat RedHat Mandriva SmoothWall **SGI** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Remote Denial of Service CVE-2005-3275	3.3	Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006 Mandriva Security Advisory, MDKSA-2006:044, February 21, 2006 SmoothWall Advisory, March 15, 2006 **SGI Security Advisory, 20060402-01-U, April 10, 2006**

Multiple Vendors
Linux kernel 2.6-2.6.14;
SuSE Linux Professional 10.0 OSS, Linux Personal 10.0 OSS;
RedHat Fedora Core4
	A Denial of Service vulnerability has been reported in 'ptrace.c' when 'CLONE_THREAD' is used due to a missing check of the thread's group ID when trying to determine whether the process is attempting to attach to itself.
	Upgrades available
	Fedora
	SUSE
	Mandriva
	DSA-1017
	DSA-1018
	DSA 1018-2
	SGI
	Currently we are not aware of any exploits for this vulnerability.
		Linux Kernel PTrace 'CLONE_ THREAD' Denial of Service
		CVE-2005-3783
			3.5	Secunia Advisory: SA17761, November 29, 2005
				Fedora Update Notification, FEDORA-2005-1104, November 28, 2005
				SuSE Security Announcement, SUSE-SA:2005:067, December 6, 2005
				SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005
				Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006
				Debian Security Advisory, DSA-1017-1, March 23, 2006
				Debian Security Advisory, DSA-1018-1, March 24, 2006
				Debian Security Advisory, DSA 1018-2, April 5, 2006
				SGI Security Advisory, 20060402-01-U, April 10, 2006

Multiple Vendors Linux kernel 2.6-2.6.15	A Denial of Service vulnerability has been reported in the 'time_out_leases()' function because 'printk()' can consume large amounts of kernel log space.	Linux Kernel PrintK Local Denial of Service CVE-2005-3857	3.5	Security Focus, Bugtraq ID: 15627, November 29, 2005 Trustix Secure Linux

	Patches available Trustix RedHat RedHat DSA-1017 DSA-1018 DSA 1018-2 **SGI** An exploit script has been published.			Security Advisory, TSLSA-2005-0070, December 9, 2005 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006 Debian Security Advisory, DSA-1017-1, March 23, 2006 Debian Security Advisory, DSA-1018-1, March 24, 2006 Debian Security Advisory, DSA 1018-2, April 5, 2006 **SGI Security Advisory, 20060402-01-U, April 10, 2006**
Multiple Vendors RedHat Fedora Core4; Linux Kernel 2.6.x	A Denial of Service vulnerability has been reported in the 'die_if_kernel()' function because it is erroneously marked with a 'noreturn' attribute. Updates available Ubuntu **SGI** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'die_if_ kernel()' Potential Denial of Service CVE-2006-0742	1.4	Security Focus, Bugtraq ID: 16993, March 5, 2006 Ubuntu Security Notice, USN-263-1 March 13, 2006 **SGI Security Advisory, 20060402-01-U, April 10, 2006**
Multiple Vendors Tony Cook Imager 0.47-0.49, 0.45, 0.41-0.43; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A remote Denial of Service vulnerability has been reported due to a failure to properly handle unexpected image data. Update to version 0.50 or later. A Proof of Concept exploit has been published.	Tony Cook Imager JPEG & TGA Images Denial of Service CVE-2006-0053	1.9	Security Focus, Bugtraq ID: 17415, April 7, 2006
Multiple Vendors Trustix Secure Linux 3.0, 2.2; Linux kernel 2.6.12 up to versions before 2.6.17-rc1	A Denial of Service vulnerability has been reported in the 'fill_write_buffer()' function due to an out-of-bounds memory error. Update to version 2.6.16.2. Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SYSFS Denial of Service CVE-2006-1055	2.3	Secunia Advisory: SA19495, April 10, 2006

Multiple Vendors
Trustix Secure Linux 3.0, 2.2;
MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2;
Gentoo Linux;
Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha; ClamAV prior to 0.88.1
	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported in the PE header parser in the 'cli_scanpe()' function, which could let a remote malicious user execute arbitrary code; format string vulnerabilities were reported in 'shared/output.c' in the logging handling, which could let remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported in the 'cli_bitset_test()' function due to an out-of-bounds memory access error.
	Updates available
	Gentoo
	Mandriva
	SuSE
	Trustix
		ClamAV Multiple Vulnerabilities
		CVE-2006-1614
		CVE-2006-1615
		CVE-2006-1630
			7.0 (CVE-2006-1614)
			10 (CVE-2006-1615)
			2.3 (CVE-2006-1630)
				Security Focus, Bugtraq ID: 17388, April 7, 2006
				Gentoo Linux Security Advisory, GLSA 200604-06, April 7, 2006
				Mandriva Security Advisory, MDKSA-2006:067, April 7, 2006
				Trustix Secure Linux Security Advisory #2006-0020, April 7, 2006
				SUSE Security Announcement, SUSE-SA:2006:020, April 11, 2006

	Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; MandrakeSoft Corporate Server 3.0 x86_64, 3.0; Jamie Zawinski XScreenSaver 4.17, 4.16, 4.14	A vulnerability has been reported because the keyboard focus is not released when xscreensaver starts, which could let a malicious user obtain sensitive information. The vendor has released version 4.18 of XScreenSaver to address this issue. Standard applications and network sniffers can be used to exploit this issue.	XScreenSaver Password Disclosure CVE-2004-2655	Not Available	Security Focus, Bugtraq ID: 17471, April 11, 2006
Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available Gentoo Ubuntu Gentoo Ubuntu ALTLinux Fedora RedHat SGI RedHat Mandrake Mandriva Debian RedHat RedHat RedHat Apple Fedora SCO SCO FedoraLegacy **SGI** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CVE-2005-0605	7.0	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:081, May 6, 2005 Debian Security Advisory, DSA 723-1, May 9, 2005 RedHat Security Advisory, RHSA-2005:412-05, May 11, 2005 RedHat Security Advisory, RHSA-2005:473-03, May 24, 2005 RedHat Security Advisory, RHSA-2005:198-35, June

				8, 2005 Fedora Update Notifications, FEDORA-2005-808 & 815, August 25 & 26, 2005 SCO Security Advisory, SCOSA-2005.57, December 14, 2005 SCO Security Advisory, SCOSA-2006.5, January 4, 2006 Fedora Legacy Update Advisory, FLSA:152803, January 10, 2006 **SGI Security Advisory, 20060403-01-U, April 11, 2006**
Multiple Vendors XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo RHSA-2005-329.html RHSA-2005-396.htm Ubuntu Mandriva Fedora Trustix Debian Sun SUSE Slackware Sun SUSE Avaya Sun 101926: Updated Contributing Factors, Relief/Workaround, and Resolution sections. NetBSD **SGI** Currently we are not aware of any exploits for this vulnerability.	XFree86 Pixmap Allocation Buffer Overflow CVE-2005-2495	3.9	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441 Fedora Update Notifications, FEDORA-2005-893 & 894, September 16, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005 Debian Security Advisory DSA 816-1, September 19, 2005 Sun(sm) Alert Notification Sun Alert ID: 101926, September 19, 2005 SUSE Security Announcement, SUSE-SA:2005:056, September 26, 2005 Slackware Security Advisory, SSA:2005-269-02, September 26, 2005 Sun(sm) Alert Notification Sun Alert ID: 101953, October 3, 2005 SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005 Avaya Security Advisory, ASA-2005-218, October 19, 2005

				Sun(sm) Alert Notification Sun Alert ID: 101926, Updated October 24, 2005 NetBSD Security Update, October 31, 2005 **SGI Security Advisory, 20060403-01-U, April 11, 2006**
Multiple Vendors xzgv Image Viewer 0.8 0.7, 0.6; SuSE Linux Professional 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 10.0 OSS, 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1	A buffer overflow vulnerability has been reported when processing JPEG files due to a boundary error, which could let a remote malicious user execute arbitrary code. SuSE Currently we are not aware of any exploits for this vulnerability.	XZGV Image Viewer Remote Buffer Overflow CVE-2006-1060	7.0	SUSE Security Summary Report Announcement, SUSE-SR:2006:008, April 7, 2006
Sun Microsystems, Inc. Solaris 10.0 _x86, 10.0, 9.0 _x86, 9.0, 8.0 _x86, 8.0	A Denial of Service vulnerability has been reported in sh(1) when creating temporary files. Updates available Currently we are not aware of any exploits for this vulnerability.	Sun Solaris SH(1) Denial of Service CVE-2006-1780	Not Available	Sun(sm) Alert Notification Sun Alert ID: 102282, April 11, 2006
Sun Microsystems, Inc. Sun Trusted Solaris 8.0, Solaris 9.0 _x86, 9.0, 8.0 _x86, 8.0	A vulnerability has been reported because the Directory Server rootDN (Distinguished Name) password may be disclosed to malicious users when privileged users run the idsconfig command or certain LDAP commands. Updates available Currently we are not aware of any exploits for this vulnerability.	Sun Solaris RootDN Password Disclosure CVE-2006-1782	Not Available	Sun(sm) Alert Notification Sun Alert ID: 102113, April 11, 2006

[back to top]

Multiple Operating Systems - Windows/UNIX/Linux/Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
ADOdb ADOdb 4.70, 4.68, 4.66	An SQL injection vulnerability has been reported due to insufficient sanitization of certain parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available Gentoo **dsa-1029** **dsa-1030** **dsa-1031** There is no exploit code required.	ADOdb PostgreSQL SQL Injection CVE-2006-0410	2.3	Secunia Advisory: SA18575, January 24, 2006 Gentoo Linux Security Advisory, GLSA 200602-02, February 6, 2006 **Debian Security Advisory, DSA-1029, April 8, 2006** **Debian Security Advisory, DSA-1030-1, April 8, 2006** **Debian Security Advisory, DSA-1031-1, April 8, 2006**
ADOdb ADOdb 4.71 & prior	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'adodb_pager.inc.php' due to insufficient sanitization of the 'next_page' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'adodb_pager.inc.php' due to the unsafe use of 'PHP_SELF,' which could let a remote malicious user	ADOdb Multiple Cross-Site Scripting CVE-2006-0806	2.3	Secunia Advisory: SA18928, February 20, 2006 **Debian Security Advisory, DSA-1029, April 8, 2006**

	execute arbitrary HTML and script code. **dsa-1029** **dsa-1030** **dsa-1031** There is no exploit code required.			**Debian Security Advisory, DSA-1030-1, April 8, 2006** **Debian Security Advisory, DSA-1031-1, April 8, 2006**
Annuaire Annuaire 1.0	Several vulnerabilities have been reported: a script insertion vulnerability was reported in 'inscription.php' due to insufficient sanitization of the 'COMMENTAIRE' parameter before using, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because it is possible to obtain the full path when certain scripts are accessed directly. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	Annuaire Script Insertion & Path Disclosure CVE-2006-1433 CVE-2006-1434	2.3 (CVE-2006-1433) 7.0 (CVE-2006-1434)	Secunia Advisory: SA19548, April 6, 2006
apt-webservice.de apt-webshop 4.0-pro, 3.0 light, 3.0 basic	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'message' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'modules.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	APT-webshop Cross-Site Scripting & SQL Injection CVE-2006-1685 CVE-2006-1687	7.0 (CVE-2006-1685) 2.3 (CVE-2006-1687)	Secunia Advisory: SA19592, April 10, 2006
Arabless.com SaphpLesson 3.0	A Cross-Site Scripting vulnerability has been reported in the 'search.php script due to insufficient filtering of HTML code from user-supplied search input before displaying, which could let a remote malicious user execute arbitrary script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	SaphpLesson Input Validation CVE-2006-1720	2.3	Security Tracker Alert ID: 1015883, April 9, 2006
aria-erp.org ARIA 0.99-6	Several vulnerabilities have been reported: a vulnerability was reported in 'genmessage.php' due to insufficient sanitization of the 'message' parameter before saving, which could let a remote malicious user execute arbitrary HTML and script code; and vulnerabilities were reported in 'docmgmtadd.php' due to insufficient sanitization of the 'description' and 'comment' parameters and in 'gencompanvupd.php' and 'gencompanyadd.php' due to insufficient sanitization of the 'name,' 'address1,' 'address2,' 'city,' 'email,' and 'web' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	ARIA Multiple Input Validation CVE-2006-1435	7.0	Security Focus, Bugtraq ID: 17411, April 10, 2006
Atomix Productions JetPhoto 2.1, 2.0, 1.0	A vulnerability has been reported due to insufficient sanitization of the 'name' and 'page' parameters before returning to users, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	JetPhoto Server Cross-Site Scripting CVE-2006-1760	Not Available	Secunia Advisory: SA19603, April 11, 2006

Autogallery Autogallery 0.x	A Cross-Site Scripting vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'pic' and 'show' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Autogallery Cross-Site Scripting CVE-2006-1750	Not Available	Secunia Advisory: SA19629, April 12, 2006
AWeb Aweb's Banner Generator 3.0 & prior	A Cross-Site Scripting vulnerability was reported in the 'banner' parameter due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	AWeb's Banner Generator Cross-Site Scripting CVE-2006-1699	1.9	Security Tracker Alert ID: 1015877, April 7, 2006
AWeb AWeb's Scripts Seller 0	A vulnerability has been reported in the 'buy.php' script because a predictable cookie is used for authentication, which could let a remote malicious user bypass the authentication process. No workaround or patch available at time of publishing, Vulnerability can be exploited through a web client.	AWeb's Scripts Seller Authorization Bypass CVE-2006-1700	7.0	Security Tracker Alert ID: 1015878, April 7, 2006
Azerbaijan Development Group AzDGVote 0	A file include vulnerability has been reported i 'admin.php,' 'vote.php,' 'view.php,' and 'admin/index.php' due to insufficient sanitization of the 'int_path' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	AzDGVote Remote File Include CVE-2006-1770	Not Available	Security Focus, Bugtraq ID: 17447, April 11, 2006
Bitweaver Bitweaver 1.3	A Cross-Site Scripting vulnerability has been reported in 'login.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Bitweaver CMS Cross-Site Scripting CVE-2006-1745	1.9	Security Focus, Bugtraq ID: 17406, April 7, 2006
Blursoft Blur6ex 0.3.462	Multiple input validation vulnerabilities have been reported including Cross-Site Scripting and SQL injection due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML, script code and SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	Blursoft Blur6ex Multiple Input Validation CVE-2006-1761 CVE-2006-1762 CVE-2006-1763	Not Available	Security Focus, Bugtraq ID: 17465, April 11, 2006

Cisco Systems Cisco Transport Controller 4.x	Multiple vulnerabilities have been reported: multiple remote Denials of Service vulnerabilities were reported when an invalid response is sent instead of the final ACK packet during the 3-way handshake; a vulnerability was reported due to errors when processing IP packets which causes control cards to reset when a specially crafted IP packet is submitted; a vulnerability was reported due to an error when processing OSPF (Open Shortest Path First) packets which causes control cards to be reset; and a vulnerability was reported in the Cisco Transport Controller (CTC) applet launcher due to 'java.policy' permissions being too broad, which could let a remote malicious user execute arbitrary code. Upgrade & Workaround information Currently we are not aware of any exploits for these vulnerabilities.	Cisco Optical Networking System & Transport Controller Multiple Vulnerabilities CVE-2006-1670 CVE-2006-1671 CVE-2006-1672	3.3 (CVE-2006-1670) 2.3 (CVE-2006-1671) 7.0 (CVE-2006-1672)	Cisco Security Advisory, cisco-sa-20060405, April 5, 2006
Clansys Clansys 1.1	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'showid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, clansys_poc, has been published.	Clansys SQL Injection CVE-2006-1708	7.0	Secunia Advisory: SA19609, April 11, 2006
Clever Copy Clever Copy 3.0	An information disclosure vulnerability has been reported due to improper restrictions to 'admin/connect.inc,' which could lead to the disclosure of sensitive information. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, adv28-K-159-2006.txt, has been published.	Clever Copy Information Disclosure CVE-2006-1718	2.3	Bugtraq ID: 17461, April 11, 2006
Design Nation dnGuestbook 2.0	An SQL injection vulnerability has been reported in 'admin.php' due to insufficient sanitization of the 'emal' and 'id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Design Nation DNGuestbook Injection CVE-2006-1710	8.0	Security Focus, Bugtraq ID: 17435, April 10, 2006
Dokeos Dokeos Open Source Learning & Knowledge Management Tool 1.6.4, 1.6 RC2, 1.5.3-1.5.5, 1.5, 1.4	An SQL injection vulnerability has been reported in 'viewtopic.php' due to insufficient sanitization of the 'topic' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Dokeos SQL Injection	Not Available	Secunia Advisory: SA19604, April 11, 2006
Gallery Project Gallery 1.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified input before using, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Vulnerability can be exploited through a web client.	Gallery Cross-Site Scripting CVE-2006-1696	2.3	Security Focus, Bugtraq ID: 17437, April 10, 2006
gfx.net N.T. 1.1.0	Several vulnerabilities have been reported: an HTML injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'username' parameter before storing in a logfile, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'index.php' due to insufficient sanitization when editing the configuration file, which could let a remote	N.T. HTML Injection & PHP Code Execution CVE-2006-1657 CVE-2006-1658	2.3 (CVE-2006-1657) 7.0 (CVE-2006-1658)	Secunia Advisory: SA19526, April 5, 2006

	malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited via a web client.			
JBook JBook 1.3	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'page' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'form.php' due to insufficient sanitization of the the 'nom' and 'mail' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	JBook Cross-Site Scripting & SQL Injection CVE-2006-1743 CVE-2006-1765	7.0 (CVE-2006-1743)	Secunia Advisory: SA19613, April 11, 2006
Jelsoft Enterprises VBulletin 3.5.1	A Cross-Site Scripting vulnerability has been reported i 'vbugs.php' due to insufficient sanitization of the 'sortorder' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	vBulletin Cross-Site Scripting CVE-2006-1673	1.9	Secunia Advisory: SA19562, April 7, 2006
Jupiter CMS Jupiter CMS 1.1.5	A Cross-Site Scripting vulnerability has been reported in 'Index.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Jupiter CMS Cross-Site Scripting CVE-2006-1679	2.3	Security Focus, Bugtraq ID: 17405, April 7, 2006
Matt WrigGuestBook 2.3.1 Secunia Advisory: SA19599	Several vulnerabilities have been reported: a vulnerability was reported in 'guestbook.pl' due to insufficient sanitization of the 'realname,' 'username,' and 'comments' parameters before using, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'guestbook.pl' due to insufficient sanitization of the 'url,' 'city,' 'state,' and 'country' parameters before using, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited via a web client; however, a Proof of Concept exploit has been published.	Matt Wright Guestbook Script Insertion CVE-2006-1697 CVE-2006-1698	2.3 (CVE-2006-1697) 2.3 (CVE-2006-1698)	Secunia Advisory: SA19586, April 10, 2006
Matthew Dingley MD News 1	An SQL injection vulnerability has been reported in 'admin.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	MD News SQL Injection CVE-2006-1755 CVE-2006-1756	Not Available	Security Focus, Bugtraq ID: 17394, April 6, 2006
MAXdev MD-Pro MAXdev MD-Pro 1.0.73, 1.0.72	An SQL injection vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'topicid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.	MAXDEV MD-Pro SQL Injection CVE-2006-1676	4.7	Secunia Advisory: SA19578, April 10, 2006

	No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.			
Multiple Vendors PostNuke Development Team PostNuke 0.761; moodle 1.5.3; Mantis 1.0.0RC4, 0.19.4; Cacti 0.8.6 g; ADOdb 4.68, 4.66; AgileBill 1.4.92 & prior	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'server.php' test script, which could let a remote malicious user execute arbitrary SQL code and PHP script code; and a vulnerability was reported in the 'tests/tmssql.php' text script, which could let a remote malicious user call an arbitrary PHP function. Adodb Cacti Moodle PostNuke AgileBill Mantis **dsa-1029** **dsa-1030** **dsa-1031** There is no exploit code required; however, a Proof of Concept exploit has been published.	ADOdb Insecure Test Scripts CVE-2006-0146 CVE-2006-0147	7.0 (CVE-2006-0146) 7.0 (CVE-2006-1047)	Secunia Advisory: SA17418, January 9, 2006 Security Focus, Bugtraq ID: 16187, February 7, 2006 Security Focus, Bugtraq ID: 16187, February 9, 2006 **Debian Security Advisory, DSA-1029, April 8, 2006** **Debian Security Advisory, DSA-1030-1, April 8, 2006** **Debian Security Advisory, DSA-1031-1, April 8, 2006**
Multiple Vendors SQuery SQuery 4.5 & prior; Autonomous LAN Party 0	Multiple remote file-include vulnerabilities have been reported in the 'LibPath' parameter due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, squery.pl.txt, has been reported.	SQuery Multiple Remote File Include CVE-2006-1610	7.0	Security Focus, Bugtraq ID: 17434, April 10, 2006
MvBlog MyBlog prior to 1.6.	Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a script insertion vulnerability was reported due to insufficient sanitization of the name and body fields when posting a comment, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Currently we are not aware of any exploits for these vulnerabilities.	MvBlog Script Insertion & SQL Injection CVE-2006-1751 CVE-2006-1752	Not Available	Secunia Advisory: SA19634, April 12, 2006
OpenVPN OpenVPN 2.0-2.0.5	A vulnerability has been reported in 'setenv' configuration directives, which could let a remote malicious user execute arbitrary code. Update to version 2.0.6. Mandriva Currently we are not aware of any exploits for these vulnerability.	OpenVPN Client Remote Code Execution CVE-2006-1629	6.0	Secunia Advisory: SA19531, April 6, 2006 Mandriva Security Advisory, MDKSA-2006:069, April 10, 2006
Oracle Corporation Oracle9i Standard Edition 9.2.0.0-10.2.0.3, Oracle9i Personal Edition 9.2.0.0-10.2.0.3, Oracle9i Enterprise Edition 9.2.0.0-10.2.0.3, Oracle10g Standard Edition 9.2.0.0-10.2.0.3, Oracle10g Personal Edition 9.2.0.0-10.2.0.3, Oracle10g Enterprise	A vulnerability has been reported due to a failure to enforce read-only privileges for user roles, which could let a remote malicious user bypass restriction accesses. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Oracle Database Access Restriction Bypass CVE-2006-1705	1.6	Security Focus, Bugtraq ID: 17426, April 10, 2006

Edition 9.2.0.0-10.2.0.3				
PHP Group PHP 4azdgvote .x, 4.2.x, 4.3.x, 4.4.x, 5.0.x, 5.1.x	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'phpinfo()' PHP function because only the first 4096 characters of an array request parameter are sanitized before returning to users, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability was reported in the 'tempnam()' PHP function due to an error, which could let a remote malicious create arbitrary files; a vulnerability was reported in the 'copy()' PHP function due to an error, which could let a remote malicious create arbitrary files; and a vulnerability was reported in the 'copy()' PHP function because the safe mode mechanism can be bypassed by a remote malicious user. Updates available Vulnerabilities may be exploited with standard PHP code; however, Proof of Concept exploit scripts have been published.	PHP Multiple Vulnerabilities CVE-2006-0996 CVE-2006-1494 CVE-2006-1608	1.9 (CVE-2006-0996) 1.9 (CVE-2006-1494) 1.6 (CVE-2006-1608)	Secunia Advisory: SA19599, April 10, 2006
PHP Group PHP 4.3.x, 4.4.x, 5.0.x, 5.1.x	A vulnerability has been reported in the 'html_entity_decode()' function because it is not binary safe, which could let a remote malicious user obtain sensitive information. The vulnerability has been fixed in the CVS repository and in version 5.1.3-RC1. Mandriva **Trustix** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Information Disclosure CVE-2006-1490	2.3	Secunia Advisory: SA19383, March 29, 2006 Mandriva Security Advisory, MDKSA-2006:063, April 2, 2006 **Trustix Secure Linux Security Advisory #2006-0020, April 7, 2006**
PHPKIT PHPKIT 1.6.1 R2	An SQL injection vulnerability has been reported in 'Include.PHP' due to insufficient sanitization of the 'contentid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	PHPKIT SQL Injection CVE-2006-1773	Not Available	Security Tracker Alert ID: 1015888, April 10, 2006
PHPList Mailing List Manager PHPList Mailing List Manager 2.10.2, 2.10.1, 2.8.12, 2.6 -2.6.4	A file include vulnerability has been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, exploit scripts, PHPList-lfi.php and phplist_2102_incl_xpl, have been published.	PHPList Local File Include CVE-2006-1746	Not Available	Security Focus, Bugtraq ID: 17429, April 10, 2006
phpMy Admin Development Team phpMyAdmin 1.x, 2.x	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of various scripts in the themes directory, which could let a remote malicious user execute arbitrary HTML and script code. Updates available Vulnerabilities can be exploited through a web client.	phpMyAdmin Cross-Site Scripting CVE-2006-1678	2.3	phpMyAdmin Security Announcement PMASA-2006-1, April 6, 2006
phpMy Forum phpMyForum 4.0	Cross-Site Scripting vulnerabilities have been reported in 'index.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	phpMyForum Cross-Site Scripting CVE-2006-1713	7.0	Security Focus, Bugtraq ID: 17420, April 10, 2006

PhpWeb Gallery PhpWebGallery 1.4.1	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, a Proof of Concept exploit has been published.	PHPWebGallery Cross-Site Scripting CVE-2006-1674 CVE-2006-1675	1.9 (CVE-2006-1674) 1.9 (CVE-2006-1675)	Security Focus, Bugtraq ID: 17421, April 10, 2006
SAXOTECH SAXoPRESS 0	A Directory Traversal vulnerability has been reported in 'apps/pbcs.dll/misc' due to insufficient sanitization of the 'url' parameter before using, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	Saxopress Directory Traversal CVE-2006-1771	Not Available	Security Focus, Bugtraq ID: 17474, April 11, 2006
Secure Ideas BASE Basic Analysis and Security Engine 1.2.4	A Cross-Site Scripting vulnerability has been reported in the 'PrintFreshPage()' function due to insufficient sanitization of various scripts, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	Basic Analysis and Security Engine Cross-Site Scripting CVE-2006-1590	2.3	Secunia Advisory: SA19544, April 6, 2006
Shadowed Works Shadowed Portal 5.7, d1 & d2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'page' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been reported.	Shadowed Portal Cross-Site Scripting CVE-2006-1701	1.9	Secunia Advisory: SA19595, April 10, 2006
ShopWeezle ShopWeezle 2.0	SQL injection vulnerabilities have been reported due to insufficient sanitization of the 'idemID' parameter in 'login.php' and 'memo.php' and in the 'index.php' due to insufficient sanitization of the 'itemgr,' 'ibrandID,' and 'album' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	ShopWeezle SQL Injection CVE-2006-1706	7.0	Security Focus, Bugtraq ID: 17441, April 11, 2006
SIRE SIRE 2.0	A file upload vulnerability has been reported due to insufficient sanitization, which could let a remote malicious user upload and execute arbitrary code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been reported.	SIRE Arbitrary File Upload CVE-2006-1704	2.3	Security Focus, Bugtraq ID: 17431, April 10, 2006
SIRE SIRE 2.0	A file include vulnerability has been reported in 'lire.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	SIRE Remote File Include CVE-2006-1703	7.0	Security Focus, Bugtraq ID: 17428, April 10, 2006

SK Soft SKForum 1.0-1.5	Multiple Cross-Site Scripting vulnerabilities have been reported in the 'areaID,' 'time,' and 'userID' parameters due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	SKForum Cross-Site Scripting CVE-2006-1661	3.3	Security Focus, Bugtraq ID: 17389, April 6, 2006
SmartISoft phpListPro 2.0	A file include vulnerability has been reported in 'config.php' due to insufficient sanitization of the 'returnpath' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	SmartISoft phpListPro Remote File Include CVE-2006-1749	Not Available	Security Focus, Bugtraq ID: 17448, April 11, 2006
SPIP SPIP 1.8.3	A file include vulnerability has been reported in 'Spip_login.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	SPIP Remote File Include CVE-2006-1702	7.0	Security Focus, Bugtraq ID: 17423, April 10, 2006
SWSoft Confixx 3.1.2	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'allgemein_transfer.php' due to insufficient sanitization of the 'jahr' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'SID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerabilities could be exploited with a web client; however, Proof of Concept exploits have been published.	SWSoft Confixx Pro Cross-Site Scripting & SQL Injection CVE-2006-1754 CVE-2006-1759	Not Available	Secunia Advisory: SA19611, April 12, 2006
The XMB Group XMB Forum 1.9.5 Final	A Cross-Site Scripting vulnerability has been reported in Flash Video due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client.	XMB Forum Flash Video Cross-Site Scripting CVE-2006-1748	Not Available	Security Focus, ID: 17445, April 11, 2006
Tritanium Scripts Tritanium Bulletin Board 1.2.3	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'register.php' due to insufficient sanitization of the 'newuser_name,' 'newuser_email,' and 'newuser_hp' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'register.php' due to insufficient sanitization of the 'newuser_realname' and 'newuser_icq' parameters before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been published.	Tritanium Bulletin Board Cross-Site Scripting CVE-2006-1768	Not Available	Secunia Advisory: SA19635, April 12, 2006

UserLand Software Manila 9.4, 9.5	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'mode' parameter in 'discuss/msgReader' and 'newsItems/viewDepartment' before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client.	Manila Multiple Cross-Site Scripting CVE-2006-1769	Not Available	Secunia Advisory: SA19636, April 12, 2006
VegaDNS VegaDNS 0.9.9	Multiple input validation vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Vulnerabilities can be exploited through a web client; however, Proof of Concept exploits have been reported.	VegaDNS Multiple Input Validation CVE-2006-1757 CVE-2006-1758	Not Available	Security Focus, Bugtraq ID: 17433, April 10, 2006
VWar VWar 1.5	A file include vulnerability has been reported in 'admin.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary PHP code. The vendor has released VWar 1.5.0 R11 to address this issue. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit has been published.	VWar Remote File Include CVE-2006-1747	Not Available	Security Focus, Bugtraq ID: 17443, April 11, 2006
XBrite XBrite 1.1	An SQL injection vulnerability has been reported in 'members.php' due to insufficient sanitization of the 'id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. Vulnerability can be exploited through a web client; however, a Proof of Concept exploit script, xbrite_poc, has been published.	XBrite SQL Injection CVE-2006-1694	7.0	Secunia Advisory: SA19602, April 10, 2006

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Phishers ring changes with phone scam: A new phishing scam has been identified by security experts that t uses a toll-free telephone number rather than a bogus website to gather online banking passwords from unwary victims.

[back to top]

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Cybercrime More Widespread, Skillful, Dangerous Than Ever: Based on evidence gathered over the last two years, the Response Team at VeriSign-owned iDefense, is convinced that groups of well-organized mobsters have taken control of a global billion-dollar crime network powered by skillful hackers and money mules targeting known software security weaknesses.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
5	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
6	Nyxum-D	Win32 Worm	Stable	March 2006	A mass-mailing worm that turns off anti-virus, deletes files, downloads code from the internet, and installs in the registry. This version also harvests emails addresses from the infected machine and uses its own emailing engine to forge the senders address.
7	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
8	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
9	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
10	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.

Table updated April 11, 2006

[back to top]

Last updated April 13, 2006